UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/085,127	03/01/2002	Yves Audebert	L741.02102	2740

24257 7590 04/16/2007
STEVENS DAVIS MILLER & MOSHER, LLP
1615 L STREET, NW
SUITE 850
WASHINGTON, DC 20036

EXAMINER	
HENNING, MATTHEW T	
ART UNIT	**PAPER NUMBER**
2131	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	04/16/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	**Application No.** 10/085,127	**Applicant(s)** AUDEBERT ET AL.	
	Examiner Matthew T. Henning	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 January 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-31* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *01 March 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

This action is in response to the communication filed on 1/31/2007.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 12/04/2006 has been entered.

Response to Arguments

Applicants' arguments filed 12/4/2006 have been fully considered but they are moot in view of the new grounds of rejection.

Furthermore, applicants' argue, with regards to the independent claims, primarily that Davis did not disclose "a communications pipe established between an HSM and a PSD that allows the HSM to communicate data or configuration changes to the PSD. The examiner points to Davis Fig. 11D, Steps 692 and 694, which generates data and sends the data to the payment server, which then sends the data to the client terminal, as seen in Fig. 11A, Steps 614-616, which passes the data to the stored value card, as is seen in Fig. 11B, Step 618. These steps meet the limitation of the claim language and as such the examiner does not find the argument persuasive.

Claims 1-31 have been examined.

Claim Rejections - 35 USC § 103

Claims 1-2, 4, 8-16, 19-20, 24-28, and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis et al. (US Patent Number 6,105,008) hereinafter referred to as Davis, and further in view of Shrader et al. (Patent Application Publication 2002/0091922) hereinafter referred to as Shrader.

Regarding claim 1, Davis disclosed a post issuance system for performing data or configuration changes within a personal security device (PSD) (Stored-Value Card See Davis Fig. 1), said system comprising: said PSD, including at least one functional application (See Davis Fig. 1 and Col. 1 Lines 45-49) and a PSD cryptographic component (See Davis Fig. 1 Element 22), a local client functionally connected to said PSD (See Davis Fig. 4 Element 204), a first server functionally connected to said local client (See Davis Fig. 4 Element 206), said PSD and said first server comprising a first component for mutual authentication (See Davis Col. 13 Line 47 – Col. 14 Line 13), at least one hardware security module (HSM), including an HSM cryptographic component complementary to said PSD cryptographic component, said at least one HSM being functionally connected to said first server (See Davis Fig. 4 Element 218 and Col. 14 Lines 14-38), a communications pipe, established between said PSD and said at least one HSM (See Davis Col. 13 Line 47 – Col. 14 Line 13), and at least one storage component that stores or generates said data or configuration changes, said at least one storage component being functionally connected to said first server (See Davis Fig. 11D), wherein: said at least one HSM comprises a controlling component that controls said data or configuration changes sent through said communications pipe to said PSD (See Davis Fig. 11D), but Davis failed to specifically disclose that the client and server comprised a first component for mutual authentication, or that the client and server mutually authenticated each other prior to the HSM sending data through said communications pipe.

Shrader teaches that in an Internet purchase system, SSL, which is well known in the art of computer security, should be used to provide secure communications between the client and the server by allowing mutual authentication, the use of digital signatures for integrity, and encryption for privacy (See Shrader Paragraphs 10-11).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Shrader in the Internet purchase system of Davis by establishing a secure channel between the client and the server prior to transaction communications. This would have been obvious because the ordinary person skilled in the art would have been motivated to allow both the client and server to verify "what entities were involved in the transaction along the transmission", as well as to protect the transmitted data from illicit access.

Regarding claim 19, Davis disclosed a post issuance method for performing data or configuration changes within a personal security device (PSD) (Stored-Value Card See Davis Fig. 1), said method comprising: establishing a communications pipe between said PSD and at least one hardware security module (HSM) (See Davis Col. 13 Line 47 – Col. 14 Line 13), wherein said PSD is functionally connected to a local client (See Davis Fig. 4 Element 204) and said at least one HSM is functionally connected to a first server (See Davis Fig. 4 Element 218 and Col. 14 Lines 14-38), mutually authenticating said PSD and said first server (See Davis Col. 13 Line 47 – Col. 14 Line 13), selecting at least one functional application within said PSD associated with existing data or configurations (See Davis Fig. 1 and Col. 1 Lines 45-49), generating or retrieving cryptographic key material from an HSM cryptographic component complementary to a cryptographic component included inside said PSD (See Davis Fig. 4 Element 218 and Col. 14 Lines 14-38), retrieving said data or configuration changes, processing said data or configuration changes by said first server (See Davis Col. 13 Paragraph 3), encrypting said processed data or configuration changes by said at least one HSM using said complementary HSM cryptographic component (See Davis Col. 15 Line 27 – Col. 16 Line 33 and Fig. 11D), routing said encrypted processed data or configuration changes through said communications pipe into said PSD (See Davis Col. 13 Paragraphs 3-4), and decrypting and processing said processed data or configuration changes by said at least one functional application using said PSD cryptographic component (See Davis Col. 13 Paragraph 5), but Davis failed to specifically disclose that the client and server comprised a first component for mutual authentication, or that the client and server mutually authenticated each other prior to the HSM sending data through said communications pipe.

Shrader teaches that in an Internet purchase system, SSL, which is well known in the art of computer security, should be used to provide secure communications between the client and the server by allowing mutual authentication, the use of digital signatures for integrity, and encryption for privacy (See Shrader Paragraphs 10-11).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Shrader in the Internet purchase system of Davis by establishing a secure channel between the client and the server prior to transaction communications. This would have been obvious because the ordinary person skilled in the art would have been motivated to allow both the client and server to verify "what entities were involved in the transaction along the transmission", as well as to protect the transmitted data from illicit access.

Regarding claim 2, Davis and Shrader disclosed a network for the establishment of said communications pipe (See Davis Fig. 4).

Regarding claims 4, and 20, Davis and Shrader disclosed at least one second server in processing communications with said first server, wherein said at least one second server includes or generates stored data or configuration changes retrievable using a PSD unique identifier (See Davis Fig. 4 Element 208, Col. 12 Paragraph 1 and Col. 15 Paragraph 2).

Regarding claim 8, Davis and Shrader disclosed a network for the establishment of said communications pipe and for functionally connecting said at least one second server to said first server, and sending means for sending said retrieved data or configuration changes from said at least one second server over said network to said first server (See Davis Fig. 4 and Col. 12 Paragraph 1 – Col. 13 Paragraph 3).

Regarding claim 9, Davis and Shrader disclosed that said first server comprises first processing means for receiving and processing said data or configuration changes, and wherein said at least one HSM comprises second processing means for further processing said data or configuration changes (See Davis Col. 13 Paragraph 3 and Col. 15 Paragraph 3 – Col. 16 Paragraph 2).

Regarding claim 10, Davis and Shrader disclosed that said at least one HSM comprises generating means for generating at least one command executable by said at least one functional application (See Col. 15 Line 63 – Col. 16 Line 33).

Regarding claim 11, Davis and Shrader disclosed that said at least one HSM comprises encrypting means for encrypting at least one command executable by said at least one functional application or said data or configuration changes, forming at least one cryptogram (See Davis Col. 16 Lines 20-22).

Regarding claim 12, Davis and Shrader disclosed sending means for sending said at least one cryptogram through said communications pipe into said PSD for processing by said at least one functional application (See Davis Col. 16 Paragraph 2 and Col. 13 Lines 41-63).

Regarding claim 13, Davis and Shrader disclosed that said at least one functional application comprises decrypting means for decrypting said cryptogram using said PSD cryptographic means, and executing means for executing said at least one command (See Davis Col. 13 Lines 52-63).

Regarding claims 14-15 and 27-28, Davis and Shrader disclosed that the network is a public or private network (See Davis Col. 6 Line 65 – Col. 7 Line 3).

Regarding claims 16 and 31, Davis and Shrader disclosed that said communications pipe is provided with a secure communications protocol (See Davis Col. 13 Lines 59-61 and Col. 20 Paragraph 1).

Regarding claim 24, Davis and Shrader disclosed using a unique identifier associated with said at least one functional application for generating or retrieving said HSM cryptographic key material (See Davis Col. 15 Line 63 – Col. 16 Paragraph 2).

Regarding claim 25, Davis and Shrader disclosed using a unique identifier associated with said at least one functional application for retrieving said data or configuration changes (See Davis Col. 12 Paragraph 1).

Regarding claim 26, Davis and Shrader disclosed that at least one command or data executable by said at least one functional application is encrypted by said at least one HSM, routed through said communications pipe into said PSD, and processed by said at least one functional application (See Davis Col. 16 Paragraph 2).

Claims 5, 6-7, 17-18, 21-23, and 29-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis and Shrader.

Regarding claims 5 and 21, Davis and Shrader disclosed a first and second server communicating information (See Davis Fig. 4) but did not specifically disclose that they had the capability of being mutually authenticated. However, mutual authentication between two communicating network elements was well known in the art at the time of invention and therefore it would have been obvious to provide the two devices with the ability of mutual authentication. This would have been obvious because the ordinary person skilled in the art would have been motivated to protect against illicit access to the contents of the devices.

Regarding claim 22, Davis and Shrader disclosed using a unique identifier associated with said at least one functional application for mutually authenticating said PSD and said first server (See Davis Col. 13 Line 47 – Col. 14 Line 39).

Regarding claims 6-7, and 23, Davis and Shrader disclosed using a functional application (See Davis Col. 7 Lines 4-6), but did not specifically disclose that the application was identified by a unique identifier. However, it was well known at the time of invention that applications had unique names which were used to identify them. Therefore, it would have been obvious for the application of Davis would have had a unique identifier used to identify the application.

Regarding claims 17-18 and 29-30, Davis and Shrader disclosed encrypting the signatures in the communications (See Davis Col. 13 Lines 59-61), but failed to disclose the type of encryption used. However, both asymmetric and symmetric encryption were well known in the art at the time of invention and therefore it would have been obvious to the ordinary person skilled in the art at the time of invention to have used either.

Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Davis and Shrader as applied to claim 1 above, and further in view of DiGiorgio et al (US Patent Number 6,385,729) hereinafter referred to as DiGiorgio.

Davis disclosed sending commands to a smartcard from the security card (See Davis Col. 14 Paragraph 3), but failed to disclose that the commands were APDU commands.

DiGiorgio teaches that APDUs are a standardized way to used to send commands to token devices (See DiGiorgio Col. 9 Paragraph 1).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of DiGiorgio in the command system of Davis by sending the commands to the stored-value card using APDUs. This would have been obvious because the ordinary person skilled in the art would have been motivated to follow the standard way of sending commands to a token device.

Conclusion

Claims 1-31 have been rejected.

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew T. Henning whose telephone number is (571) 272-3790. The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Matthew Henning
Assistant Examiner
Art Unit 2131
4/12/2007

04/11/2007
SYED ZIA
PRIMARY EXAMINER
AU 2131.